The Security Implications Of The Internet Of Things

Dr. Chris Rose, Rosenco, Inc, Florida, USA

ABSTRACT

The Internet of Things connects various electronic devices and these can range from the expensive, such as cars or computers, to the mundane, such as toasters or light bulbs and this creates a major security problem. While attention is paid to the complex expensive items, the inexpensive items, although connected to the same network, are often overlooked. With a desperate race to produce more for less and to connect more items to the network, these inexpensive items are overlooked, never updated and in many cases, are downright dangerous when connected to a network and this makes the Internet insecure for everyone else.

Keywords: Internet of Things; IoT; Network; Security; Hacking

BACKGROUND

It is estimated by Gartner that there are over 5.5 million new Internet of Things (IoT) devices connected to the Internet every day, these include cars, hospital equipment and even toasters and kettles and these will total 6.4 billion by the end of the year. Furthermore, it is expected that approximately 20 billion IoT devices will be connected to the Internet by 2020 (Palmer, 2016). In fact, in the second quarter, U.S. telephone carriers added more cars than phones to their networks therefore for the first time they are now adding more IoT connections than they are adding phones. According to statistics by Chetan Sharma Consulting, counting all U.S. carriers, 1.2 million phones, and 900,000 tablets were added to networks but 1.4 million cars were connected to cellular networks. AT&T has added cars faster than phones for seven consecutive quarters and will soon reach 10 million connected cars. However, what many do not realize is that it is the car companies that are pushing to get these live cellular connections, so that they can monitor their cars, update the software in the car and get feedback to improve future models (Lawson, 2016).

In the mid-1990s, we had a crisis of insecurity in personal computers, with both operating systems and applications having multiple vulnerabilities and there apparently was no way they could ever be patched. At that time, most companies were attempting to maintain the secrecy of their vulnerabilities and were taking their time releasing updates. By the time the updates came out it was almost impossible to get users to install the updates. Over time this has changed, due to a combination of full disclosure and automatic updates, so we now have an automatic updating system, and although not perfect, it is much better than what prevailed in the 1990s.

However, today we have a much more serious problem since IoT devices are all connected to the Internet. If you compare the power of a router or modem today, they are even more powerful than the personal computers at that time and yet the IoT devices contain these relatively powerful computer chips. However, the industries that produce these types of devices are even less proficient at solving the problem than the 1990s-computer industry. Today it will be a worse problem, because we now have a completely different Internet-connected world (Schneier, 2016).

IoT PROBLEM

The major problem we face with the IoT is that computing is now embedded into the hardware itself and although these embedded systems have multiple vulnerabilities there is no good method of patching them. The embedded system market is much different from the computer market. An embedded system is typically powered by a special type of computer chip made by companies, such as Broadcom or Marvel, they are cheap and have very little profit.

Manufacturers try to differentiate these computer chips not only by price but they also try to differentiate by features and bandwidth.

Usually, these devices are powered by a version of Linux as well as some open-source and proprietary drivers and components but little engineering is done before shipping and there is not much motivation to update their boards until necessary. The device manufacturers choose the chip based on the price and the features, then take this to build their product, whether it is a modem, router or other type of embedded device. Whoever puts their brand name on the box might add a few features, a user interface, check to make sure everything is working, and then they are finished. If we look at this scenario it is easy to see that no one company has any incentive or perhaps does not even possess the expertise or ability to patch the software once it reaches the consumer. The manufacturer of the chip would already be busy working on the next version of their chip, trying to make it faster, cooler, cheaper, and more efficient while the producer of the equipment would already be busy working on their next model. Therefore, keeping older devices maintained is not a priority. In fact when it ships, it is often shipping with old software even while the device is new (Schneier, 2016).

SECURITY BREACHES

If one night you put your well-behaved toddler to bed and the next morning they start spewing profanity, no, they are not possessed and no, you do not need an exorcist, the usual reason is that a hacker has broken into your baby monitor and webcam and has been teaching the toddler profanity all night.

An IoT search engine, Shodan, launched a new section and this lets users browse vulnerable webcams. All types of images are available, from kitchens to garages, children, schools, colleges, banks, gardens, cash registers, swimming pools and even marijuana plantations. They are vulnerable because they all use the Real Time Streaming Protocol which is open at port 554 and have no password or other method of authentication in place. This highlights the pathetic state of security on the IoT but the problem will persist because webcam manufacturers are in a race to the bottom and consumers do not perceive that there is value in security and privacy and are not willing to pay for this. Therefore, the webcam manufacturers slash costs to maximize profits, usually on very thin margins, since many webcams sell for as little as $20 today. The consumers state they are really not supposed to know about cybersecurity, while the vendors will not help because it costs money. If consumers were making these decisions and these decisions only affected them, it would not be that important, but most do not comprehend the consequences of insecure IoT devices. These devices make the Internet insecure for everyone else and it is only a matter of time before a botnet will use vulnerable webcams to launch a DDoS attack or malware will use these same webcams to infect a connected home (Porup, 2016).

At a recent demonstration, BlackBerry wanted to demonstrate that people are moving away from server attacks and are now attacking user end-points, so they hacked a connected kettle. Once they gained access to the kettle, they were than able to gain access to the secure network and showed that in an enterprise, setting hackers could easily gain access to what was thought to be a secure network. The entire hack only took 10 minutes and since the kettle has no memory itself, absolutely no evidence was left behind and all traces disappeared once the device was turned off (Goovaerts, 2016).

Security firm Bitdefender examined a smart socket which allows the user to control the plugs over the Internet via Wi-Fi. A user can turn the plug on and off using an app on their smartphone. The outlet also sends an email to the user whenever the state changes. Bitdefender found that the outlet comes with a weak username and password, which does not force the user to change. It also communicates unencrypted so by eavesdropping on the Wi-Fi everything can be seen. They found they could hijack the socket, steal the email address and password, they could inject commands into the software coding and control the product anywhere over the Internet. A hacker could install malicious firmware into these smart sockets turning them into a botnet to launch cyberattacks. In addition, computers and other electronics connected to the same Internet connection would now be vulnerable (Kan, 2016).

CONNECTED VEHICLES

Tesla is considered to be the gold standard of connected cars but researchers at a recent Def Con hacker conference demonstrated that they were able to deceive Tesla's sophisticated sensors and make it hit an object that it would usually detect in its path. In a normal state the car would not move but when they jammed the sensor it moved. Although this was just a proof of concept and not real-world conditions, it showed that in a few years someone could make a device that could jam sensors in a nearby car (Szoldra, 2016).

Recently in Nice, France, a terrorist drove a truck into a crowd killing 84 people. However, emerging technology in the form of autonomous vehicles could even remove the terrorist from the attack. An autonomous truck is much the same as a self-driving car using Wi-Fi and artificial intelligence. Increasingly more vehicles have access to the Internet and someone can hack into that signal. If a truck communicates speed, location, fuel and other parameters to headquarters someone could intercept that and trick the truck into thinking that they were fleet headquarters. And the ironic fact is that it is the truck's safety features that provide the most opportunities for hackers because the same technology that allows an autonomous vehicle to wirelessly inform another that it is about to come around a corner would be the point of greatest vulnerability for the hacker. Any large 40-ton vehicle can be taken over and be driven into anything, and if it is a fuel tanker, it could cause a really big explosion (Bukszpan, 2016).

The only reason these flaws are not being exploited now is hackers currently have very little interest even though these devices are easy to hack. If you think about a car you realize that integrity and vulnerability threats are much worse than confidentiality since there can actually be risks to life and property. If a hacker used the systems in a connected car for surveillance on the occupants, that would be bad but it would be catastrophic if they disabled the brakes. Eventually, hackers will figure out how to upload ransomware to the computer system of a car but it is not just consumers, an infected IoT device on any corporate network would be the gateway for hackers. (Palmer, 2016).

IoT SECURITY

Since everything is now getting connected to the Internet, this creates an additional security risk for society as a whole. As infrastructure, such as dams and power plants and as governments, cities, houses and cars get connected there is an increasing risk of a catastrophe. We are reaching the point where our systems are getting too big to fail, but eventually they will.

Security experts have continually argued that IoT devices pose a security risk but very little has been done to solve the dilemma. The root of the problem is that IoT is so new that standards do not exist and neither manufacturers or vendors will spend money to solve a problem for a product that might never make a profit. This strategy depends on updates being provided by patches, either by being downloaded or by replacing the device, but realistically they will never be patched. The way a router is patched today is by replacing one router with a newer model. Many devices are frequently patched but in reality, many times it is through replacement. We might get a new phone every 18 months or a laptop every two years but realistically with many devices this is not going to happen. The home appliance market just is not the same as the consumer electronics market, everything is different. There are different economics, different security cycles and different life cycles (Palmer, 2016).

A major technological hurdle is also the Public Key Infrastructure (PKI). This was created in the 1970s to secure communication between two human parties and was never meant to handle 50 billion devices on massive networks. In the 1990s, everyone was focused on data in motion or the communication between two parties. What they focused on instead was data at rest and this is the major cause of security problems today. PKI was designed for people to encrypt and share a secret message and if one of the parties believed the message was compromised they could simply go and generate a new key pair and register the public key. But by concentrating on communication, there is no way to audit the chain of custody of the data or the data hosted by various parties in differing environments along the way. It is a failing strategy to base the security of a network on the integrity of encryption keys and their administrators. Data must be examined throughout its entire lifetime and not just the secure transmission while it is in motion between devices which will be of no value if the device itself is compromised. In machines, data begins and ends at rest while passing through various relay activities e.g. user access, authentication,

interaction with hardware and myriad numbers of activities and any truly effective solutions must continuously monitor the state of a network's entry points and the data within (Gault, 2016).

CONCLUSION

The Internet of Things (IoT) is enabling a revolution in technology by connecting various digital devices for increased speed, efficiency and convenience. These devices can be as varied as in the automotive or aviation industries, or in healthcare or energy, but with sensitive data now more accessible online, this means there are more endpoints available to attack, therefore security cannot be an afterthought (Gault, 2016).

In reality, there are very few applications that can monitor IoT devices to warn of any new threat or anomaly or inform you of recent compromises. Because of this IoT threats will continue to multiply as more devices are adopted at home and in the workplace. A new connected device solves a problem but it is this utility that makes IoT more vulnerable. We often know very little about the hardware or software used to solve the problem. IoT devices are simple but they often share Wi-Fi credentials and this is one of the greatest problems. In addition, there are too many orphan devices, those that are no longer supported because the manufacturer has gone out of business, but the device is still left unpatched, ignored yet connected to a network (Brandon, 2016). Until there is some incentive to create standards for embedded devices, to develop and deploy mandatory patch management systems for these devices, force some level of encryption on every IoT device, and remove outdated devices, there will always be increased risk for the entire Internet whenever one of these IoT devices connects to the Internet.

AUTHOR BIOGRAPHY

Dr. Chris Rose, a consultant with Rosenco, Inc., Florida, has been teaching both online and ground-based undergraduate and graduate level courses for over 18 years at various universities. A graduate of Florida International University and Nova Southeastern University, his current areas of interest are the Internet of Things and Cryptographic Digital Currencies.

REFERENCES

Brandon, J. (2016) CSO. Security concerns rising for Internet of Things devices. Retrieved 08/28/2016 from http://www.csoonline.com/article/3077537/internet-of-things/security-concerns-rising-for-internet-of-things-devices.html

Bukszpan, D. (2016) CNBC. Could autonomous trucks be the next weapon for terrorists? Retrieved 08/26/2016 from http://www.cnbc.com/2016/07/21/could-autonomous-trucks-be-the-next-weapon-for-terrorists.html

Gault, M. (2016) TechCrunch. Rethinking security for the Internet of Things. Retrieved 08/28/2016 from https://techcrunch.com/2016/05/06/rethinking-security-for-the-internet-of-things/

Goovaerts, D. (2016). WirelessWeek. BlackBerry Hacked a Tea Kettle and It Was Scarier Than You'd Think. Retrieved 8/29/2016 from https://www.wirelessweek.com/blog/2016/07/blackberry-hacked-tea-kettle-and-it-was-scarier-youd-think

Kan, M. (2016). CIO.com. One smart plug isn't so bright when it comes to security. Retrieved 8/27/2016 from http://www.cio.com/article/3109536/security/one-smart-plug-isnt-so-bright-when-it-comes-to-security.html

Lawson, S. (2016) Computerworld. IoT is now growing faster than smartphones. Retrieved 08/27/2016 from http://www.computerworld.com/article/3106446/internet-of-things/iot-is-now-growing-faster-than-smartphones.html

Palmer, D. (2016) ZDNet. The first big Internet of Things security breach is just around the corner. Retrieved 08/28/2016 from http://www.zdnet.com/article/the-first-big-internet-of-things-security-breach-is-just-around-the-corner/

Porup, J. (2016) ArsTechnica. Retrieved 8/27/2016 from http://arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/

Schneier, B. (2016) Wired. The Internet of Things is wildly insecure – and often unpatchable. Retrieved 08/26/2016 from http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and- thats-a-huge-problem/

Szoldra, P. (2016) Business Insider. Hackers show how they tricked a Tesla into hitting objects in its path. Retrieved 08/29/2016 from http://www.businessinsider.com/defcon-tesla-jamming-spoofing-autopilot-2016-8